MSTP

Windows 2003 Architecture

Concepts and Design

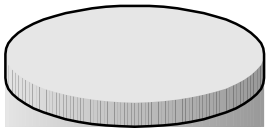
Course Outline

MSTP

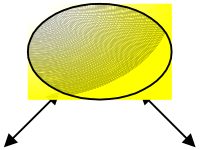
- Intro to Active Directory (AD)
- AD Architecture
  - Flexible Single Master Operations (FSMO) Roles
- AD Replication Topologies
  - AD Replication Concepts & the Knowledge Consistency Checker (KCC)
  - Intra/Inter-site Replication topologies
  - Three Hop Rule
- Windows 2003 Service/Exchange Integration with AD

Graphical Symbols

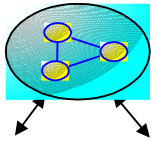
MSTP



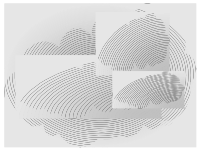
Site



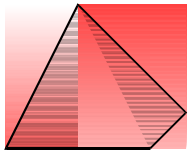
Site Link



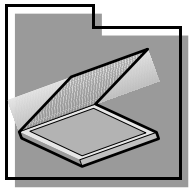
Site Link Bridge



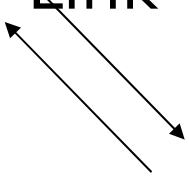
Fore t



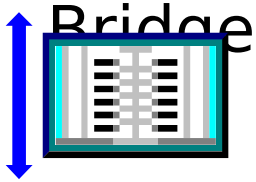
Doma in



Organizational Unit



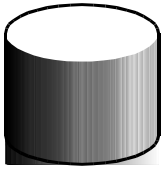
Replication Link



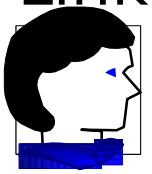
Subnet

Domain Controller

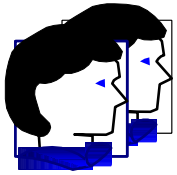
Client



Naming Context / Partition



User



Group

Intersite Link

Intrasite Link

What Is Active Directory?

MSTP

- Active Directory Architecture
  - Distributed Database containing objects such as
    - Users
    - Computers
    - Printers
  - Integrated Implementation of DNS, DHCP, LDAP and Kerberos
  - Two Modes of operation
    - Native
    - Mixed Mode

Domain Differences

MSTP

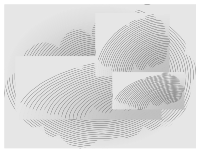
Capability	NT 4.0	Windows 2003
Unit of replication	Object	Attribute
Size	40,000 objects	1,000,000+ objects
Naming/Resolution	NetBIOS(WINS)	DNS
Delegation of administration	Create new domain	Delegate within domain using OUs

Active Directory Components

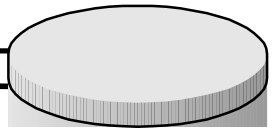
MSTP

- Forest
- Tree
- Domain
- Organizational Unit

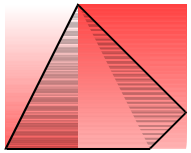
  * Sites



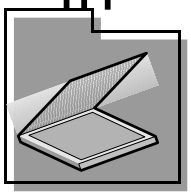
Forest



Site



Domain



Organizational Unit

Forest

- Forest
  - A group of one or more Active Directory Trees that trust each other via two-way transitive trusts. All trees in the forest share a common schema, configuration and Global Catalog (GC).

Tree

MSTP

- Share a common Schema, Configuration and Global Catalog
- Contiguous Namespace within the Tree

Domain

MSTP

- Domain- A group of computers that share a security policy and a user account database. (Administrative Boundary)

Organizational Unit (OU)

MSTP

- A container object in Active Directory used to separate computers, users, and other resources into logical units.
- An Organizational Unit is the smallest entity to which Group Policy can be applied

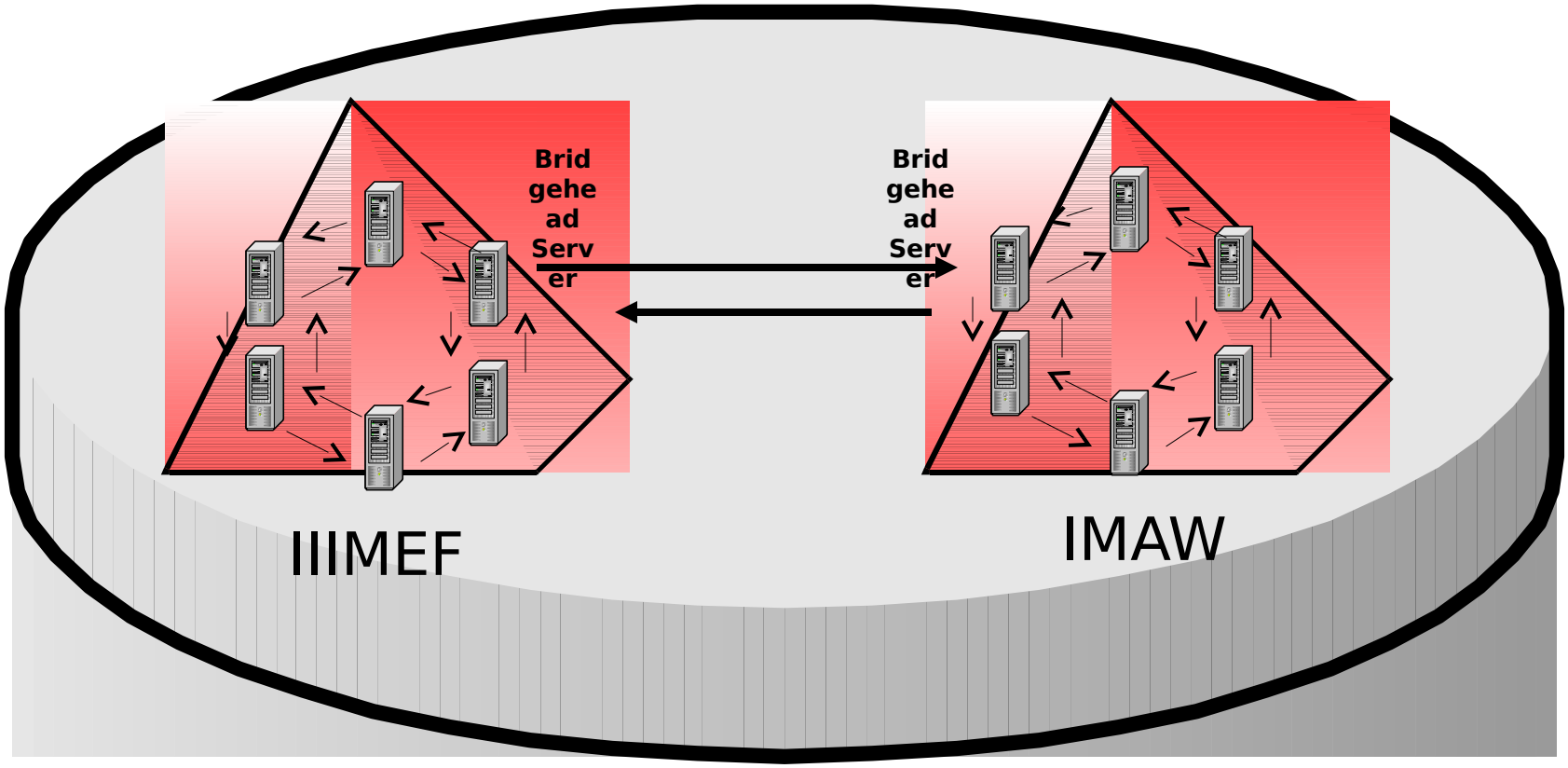
Sites

MSTP

- Site
  - A region of your network with high bandwidth connectivity, and by definition is a collection of well-connected computers
  - Defined by IP subnets
  - Computers within a site are usually located physically close together
  - When a user logs onto the network they will use services provided by servers in their site first to reduce WAN traffic

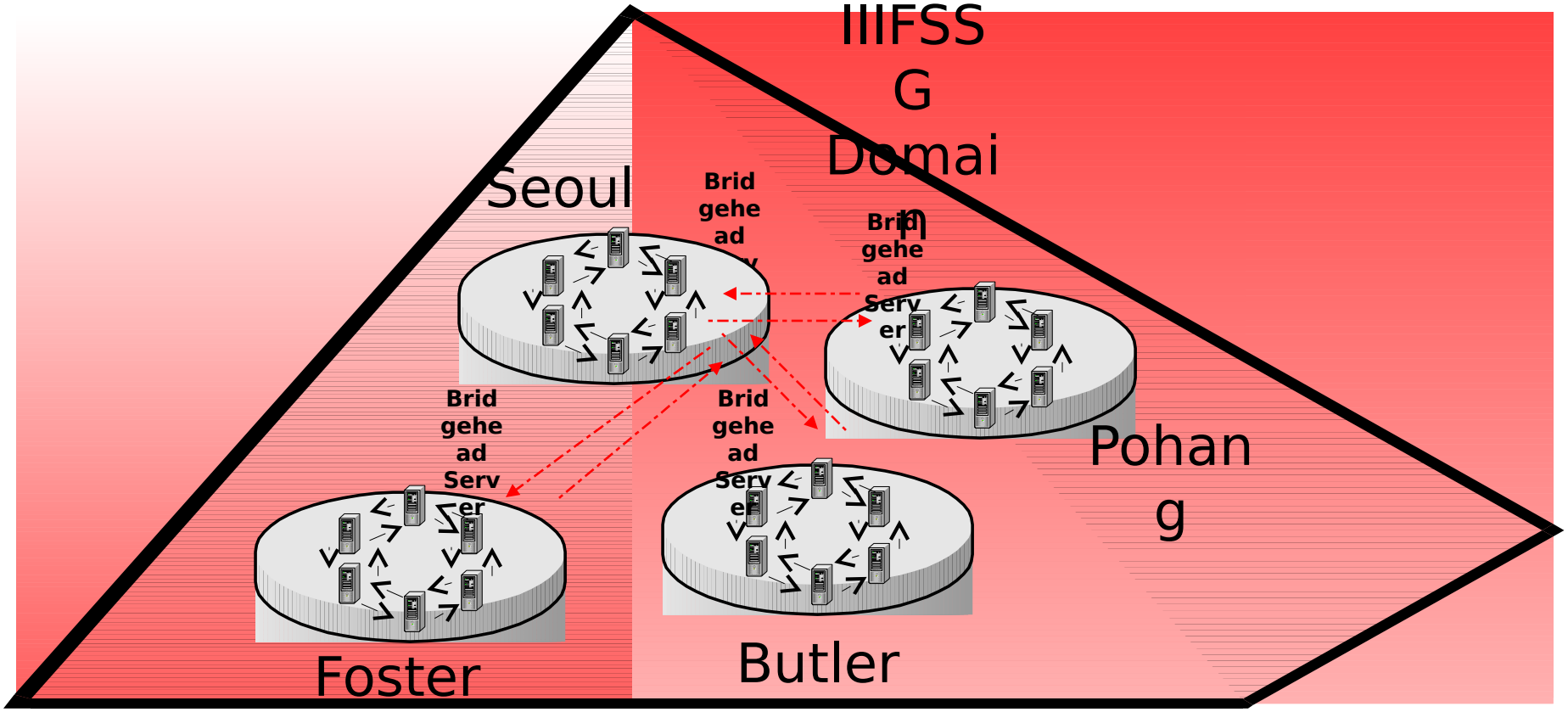
Site and Domain Relationships

MSTP



Site and Domains

MSTP



Groups

MSTP

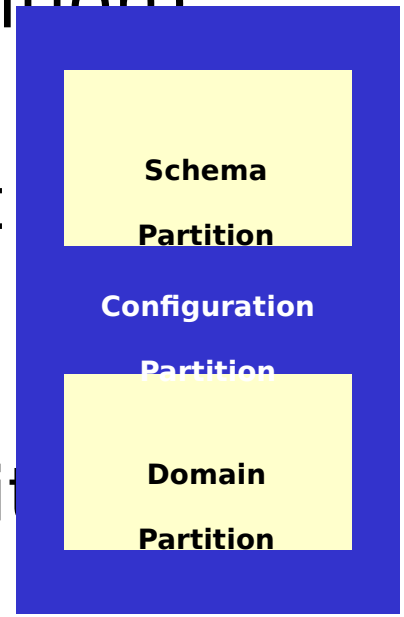
- Domain Local
  - Can contain objects from the same domain or other domains
- Global Group
  - Can contain objects from the same domain
- Universal Group
  - Can contain objects and users from the same domain or any other domain in the Forest
  - Only available in Native Mode

- Policy is applied to Organizational Units
- Permissions are applied to Groups

Active Directory Partitions

MSTP

- The Active Directory Database is divided into three partitions
  - Schema Naming Context (Partition)
    - One per Forest
  - Configuration Naming Context (Partition)
    - One per Forest
  - Domain Naming Context (Partition)
    - As many as you have Domains



FSMO Roles

MSTP

- Schema Master (Enterprise wide)
- Domain Naming Master (Enterprise wide)
- Primary Domain Controller (PDC) Emulator (Domain wide)
- Relative Identifier (RID) Master (Domain wide)
- Infrastructure Master (Domain wide)

Schema Master

MSTP

- Schema Master (Enterprise wide)

  - Manages changes to properties of objects in the Active Directory.

  Ex.

  If you add the attribute of Rank to the user object you change the schema. If you change the users rank from Maj to LtCol you are only modifying the value of the attribute not the schema.

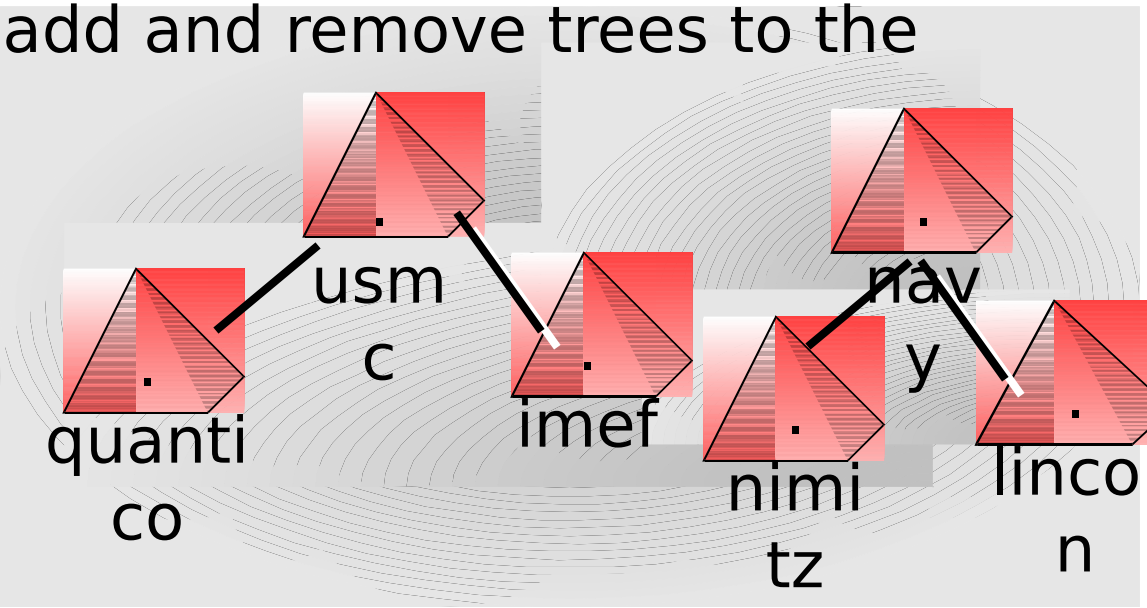
Domain Naming Master

MSTP

- Domain Naming Master (Enterprise wide)

  -Controls changes to the name space of the forest

  The Domain Naming Master is the machine that will be able to add and remove trees to the forest.



PDC Emulator

MSTP

- PDC Emulator (Domain wide)

  -Used to provide services to non-windows 2003 clients.

  Services include the processing of password changes from both users and computers, Replicating updates to Backup Domain Controllers (NT) and running the Domain Master Browser for the Legacy Browser services on older systems.

  -A PDC Emulator is only needed when supporting legacy clients.

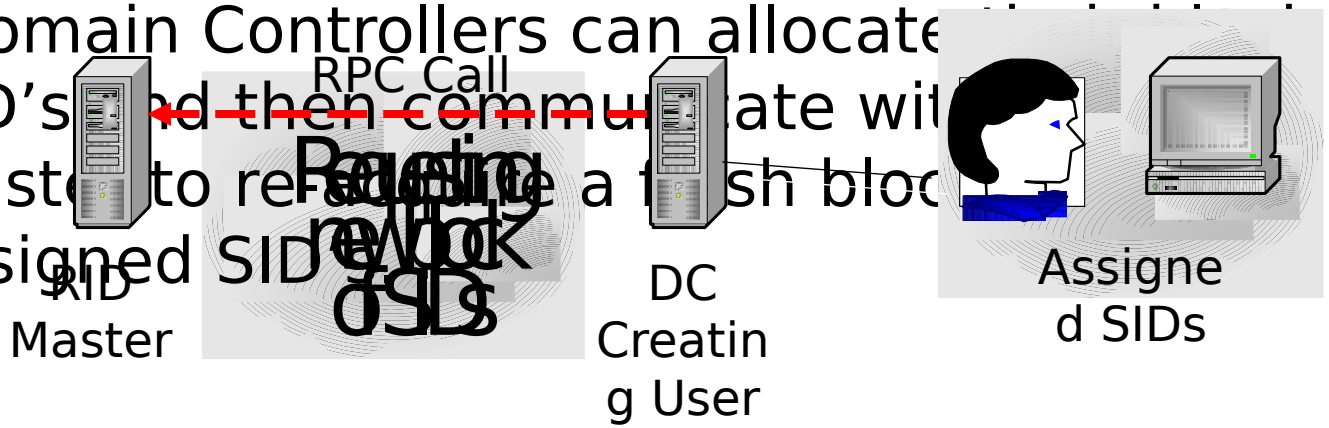
RID Master

MSTP

- RID Master (Domain wide)

  -Keeps all Security ID's (SID's) in the domain unique by allocating a block of Globally Unique Identifiers to the DCs creating objects requiring Security Identifiers such as Users and Computers.

  -Domain Controllers can allocate their block of SID's and then communicate with the RID Master to request a fresh block of assigned SIDs



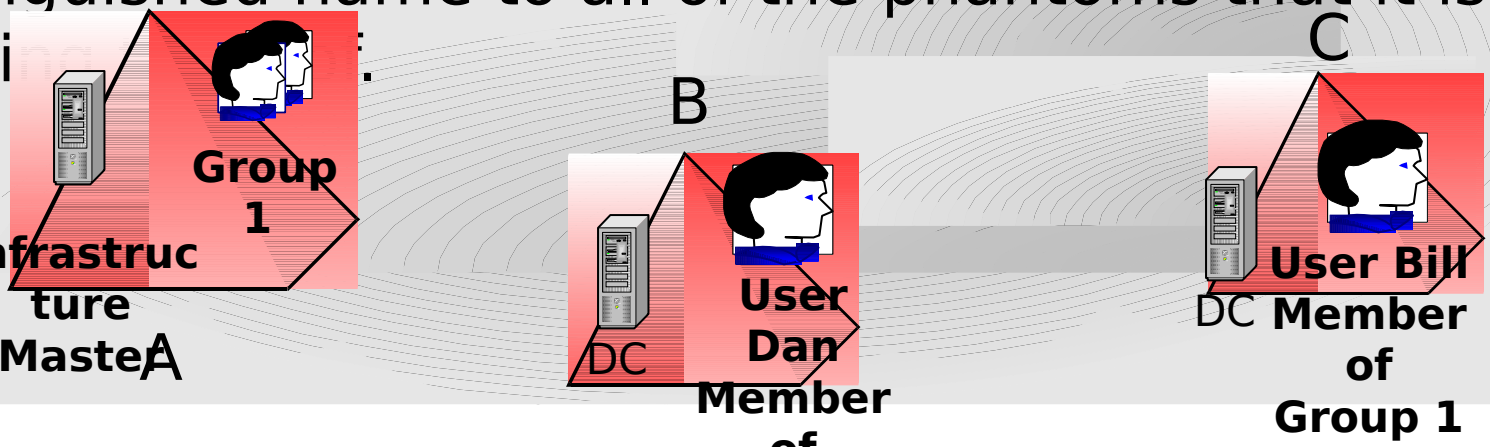
Infrastructure Master

MSTP

- Infrastructure Master (Domain wide)

  -Keeps track of all phantoms or objects in another name space of the forest

Ex. An object on a server in another domain is renamed. The distinguished name is changed but not the SID. The Infrastructure master updates the distinguished name to all of the phantoms that it is keepi[illegible].



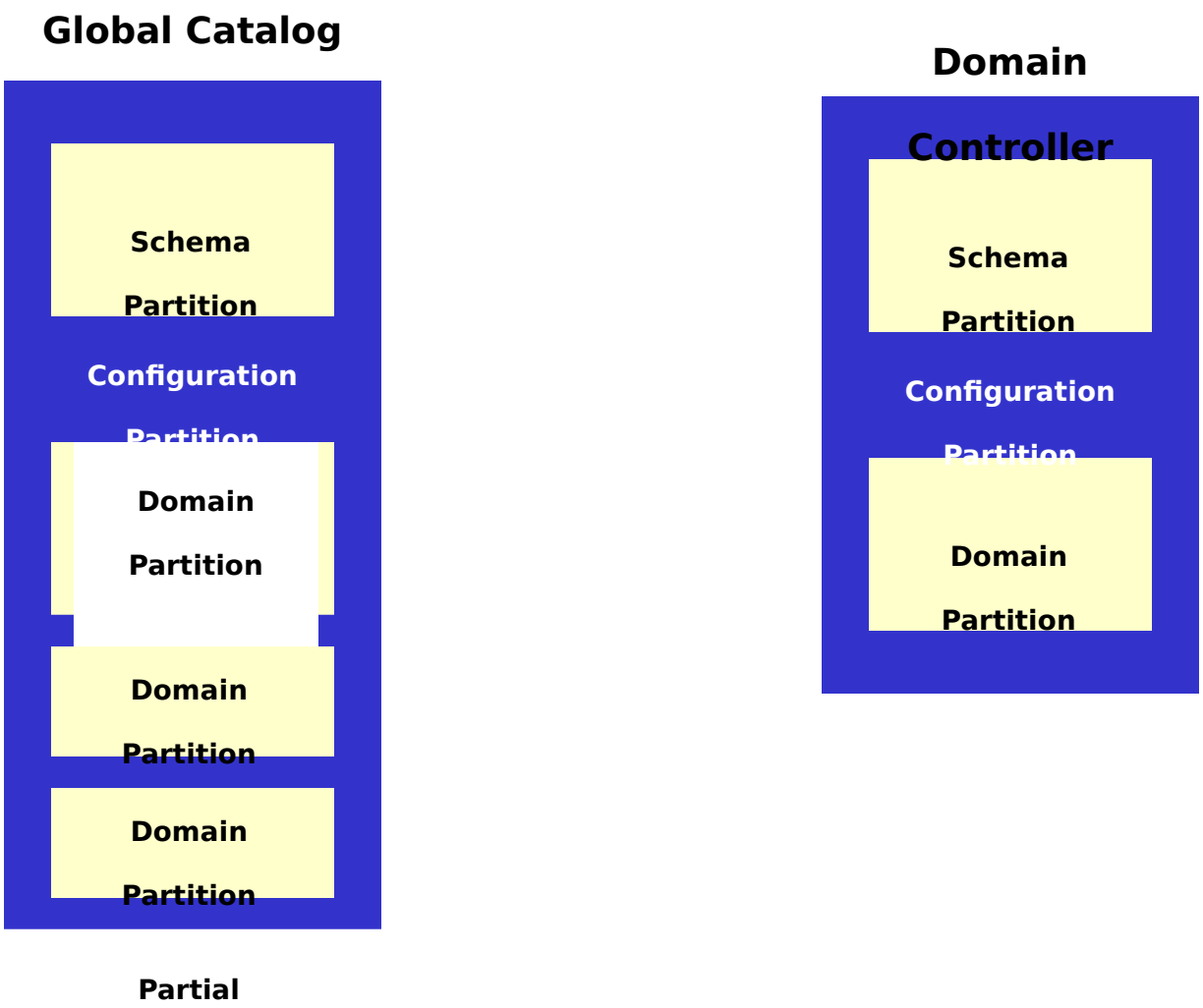
Global Catalog (GC)

MSTP

- Contains a full replica of all directory objects in its host domain plus a partial replica of all directory objects in all domains in the forest.
- Used to speed up searches
  - A GC query is much faster than an AD query
- Used by the User Logon Process
  - At logon a user will check with the GC to see if they are members of any Universal Groups
  - Also used at logon if the user logs on using the User Principle Name method username@domain.com

GC vs. DC

MSTP


Global Catalog
Schema Partition
Configuration Partition
Domain Partition
Domain Partition
Domain Partition
Partial
Domain Controller
Schema Partition
Configuration Partition
Domain Partition

AD Replication and Link Generation

MSTP

- Knowledge Consistency Checker (**KCC**)
  - Runs by default every 15 minutes
  - May be started manually if desired
  - Defines incoming replication only on each server
  - Configuration and Schema share a replication topology
  - Domain topology will be setup if you span sites
  - Global catalog topology will also be created through the forest

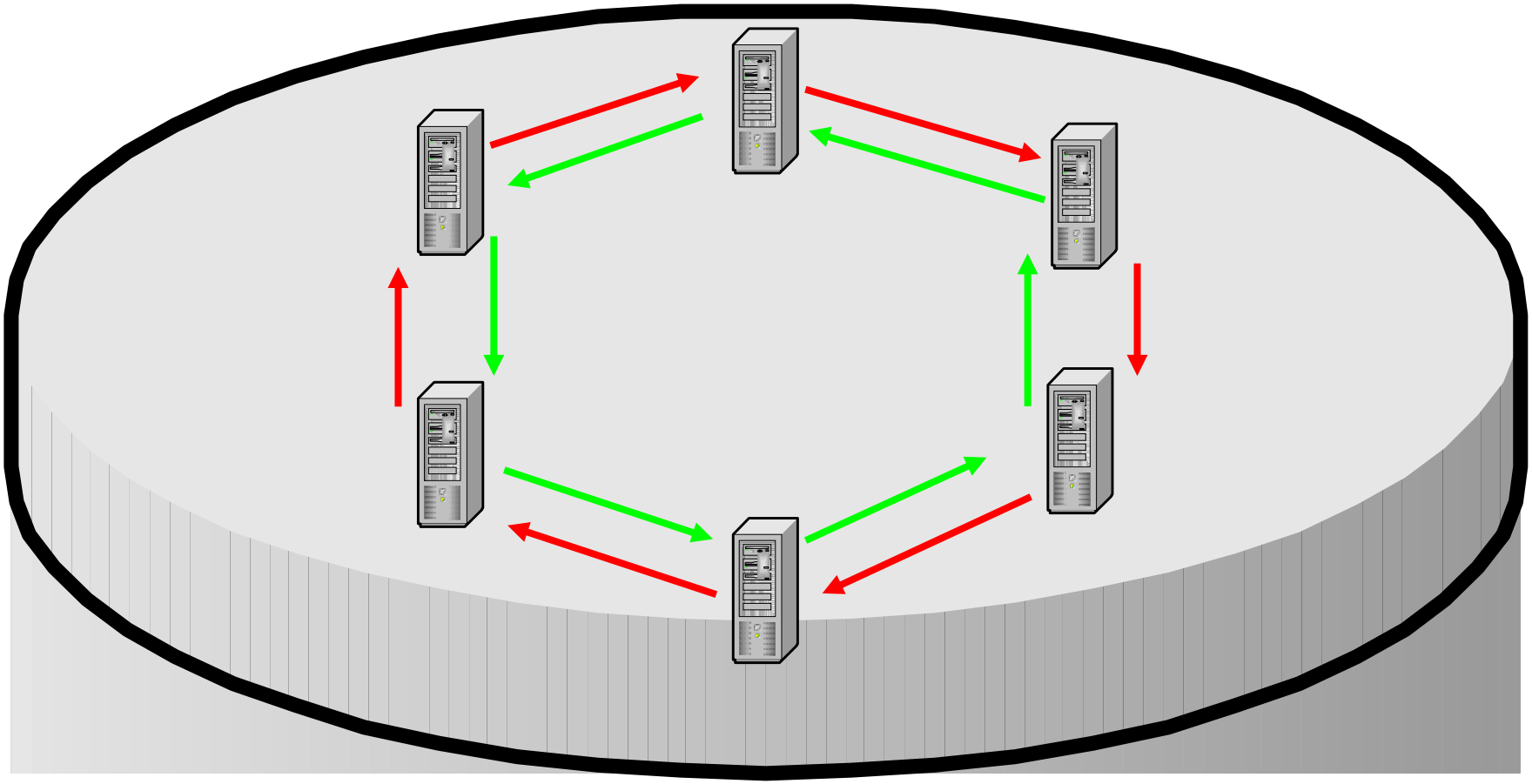
AD Replication Intra-Site

MSTP

- Intra-Site (Inside of a site) sets up replication partners automatically
  - Automatic Replication
  - If no changes occur AD replicates every 6 hours
  - Every DC must be within three hops from every other DC
  - Remote Procedure Call (RPC) is the only replication transport that can be used intra-site

Intra-Site Replication

MSTP



Bi-Directional Ring

Three Hop Rule

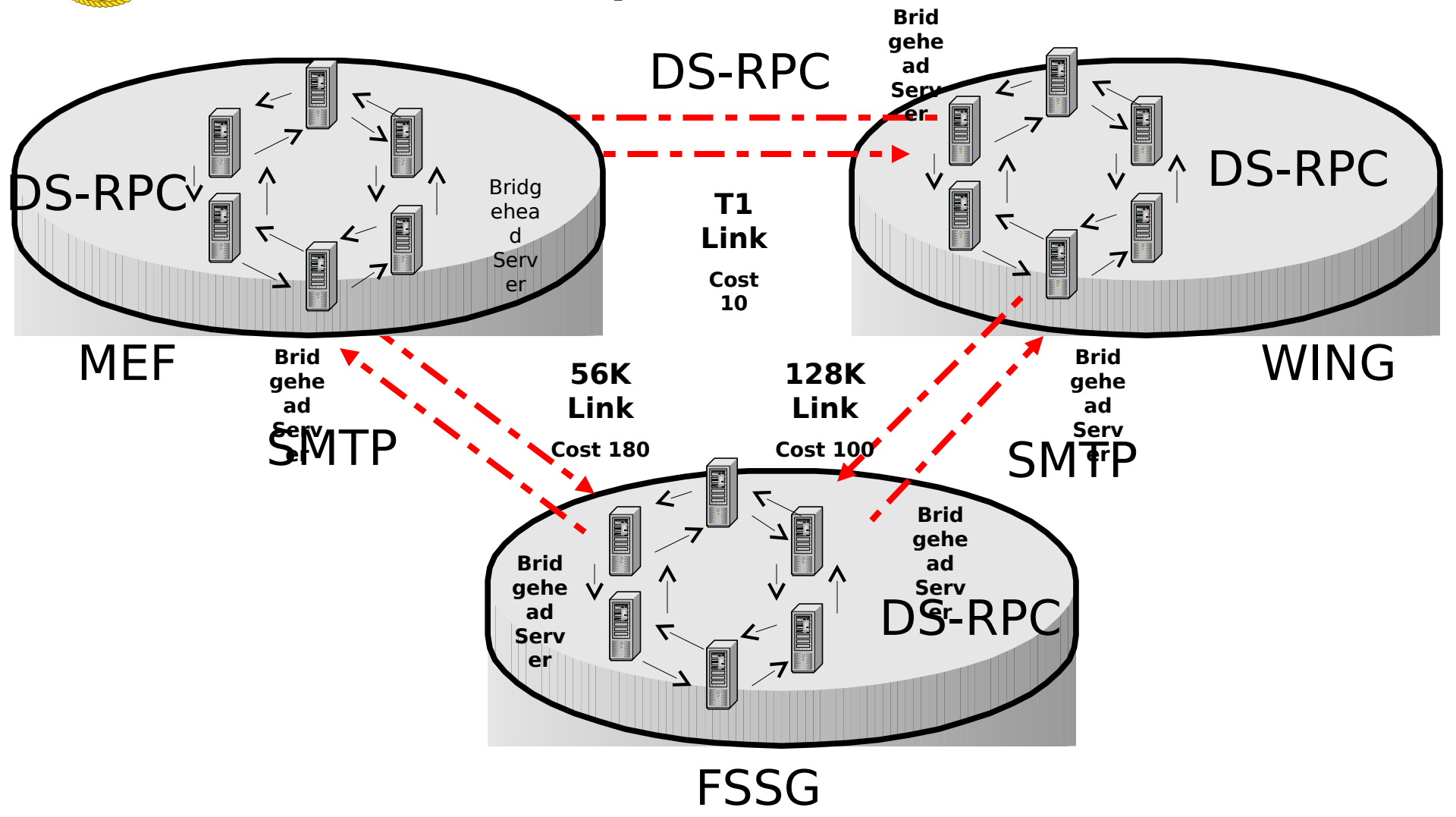
AD Replication Inter-Site

MSTP

- Inter-Site Replication (Site to Site)
  - The site link must be created by an administrator and the KCC will automatically use these links
  - Scheduled replication
  - RPC and SMTP available Inter-Site

Intra vs. Inter-site Replication

MSTP



Site Links

MSTP

- Logically created connection between sites that reside on an underlying physical network
  - Sites do not have to be physically connected to replicate
  - Costs can be assigned to site links

Site Links

- Four properties of site links
  - Name
  - Cost
  - Schedule
    - Replication time window
  - Transport Protocol
    - RPC
    - SMTP

Site Links

MSTP

- When Multiple routes exist the KCC will add costs together
- Schedule windows on each end of the site link must coincide or replication will not occur
- Be cautious when setting up new inter-site links and setting costs:
  - Ex. Cost of 50 and instead you type 5

Site Links and RPC

MSTP

- Synchronous real-time link
- Domain Partition must use RPC
- Uses the Replication Available / Not Available Site Link settings to schedule replication
- Point to Point
- Low-speed

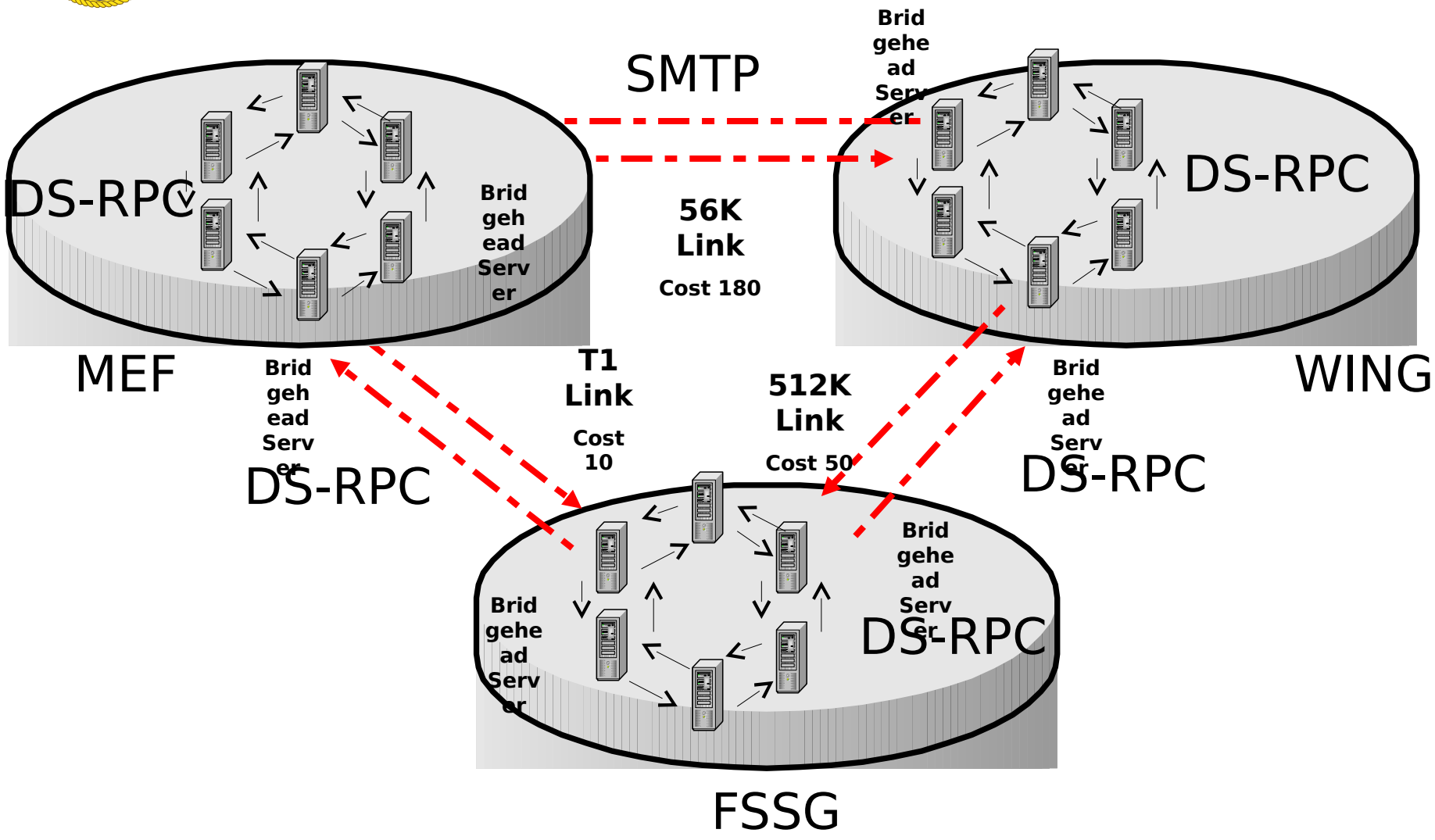
Site Links and SMTP

MSTP

- Encrypt and e-mail updates across the link
- Uses certificates to validate and secure
- Global catalog
- Schema Partitions
- Configuration Partitions

Site Links

MSTP



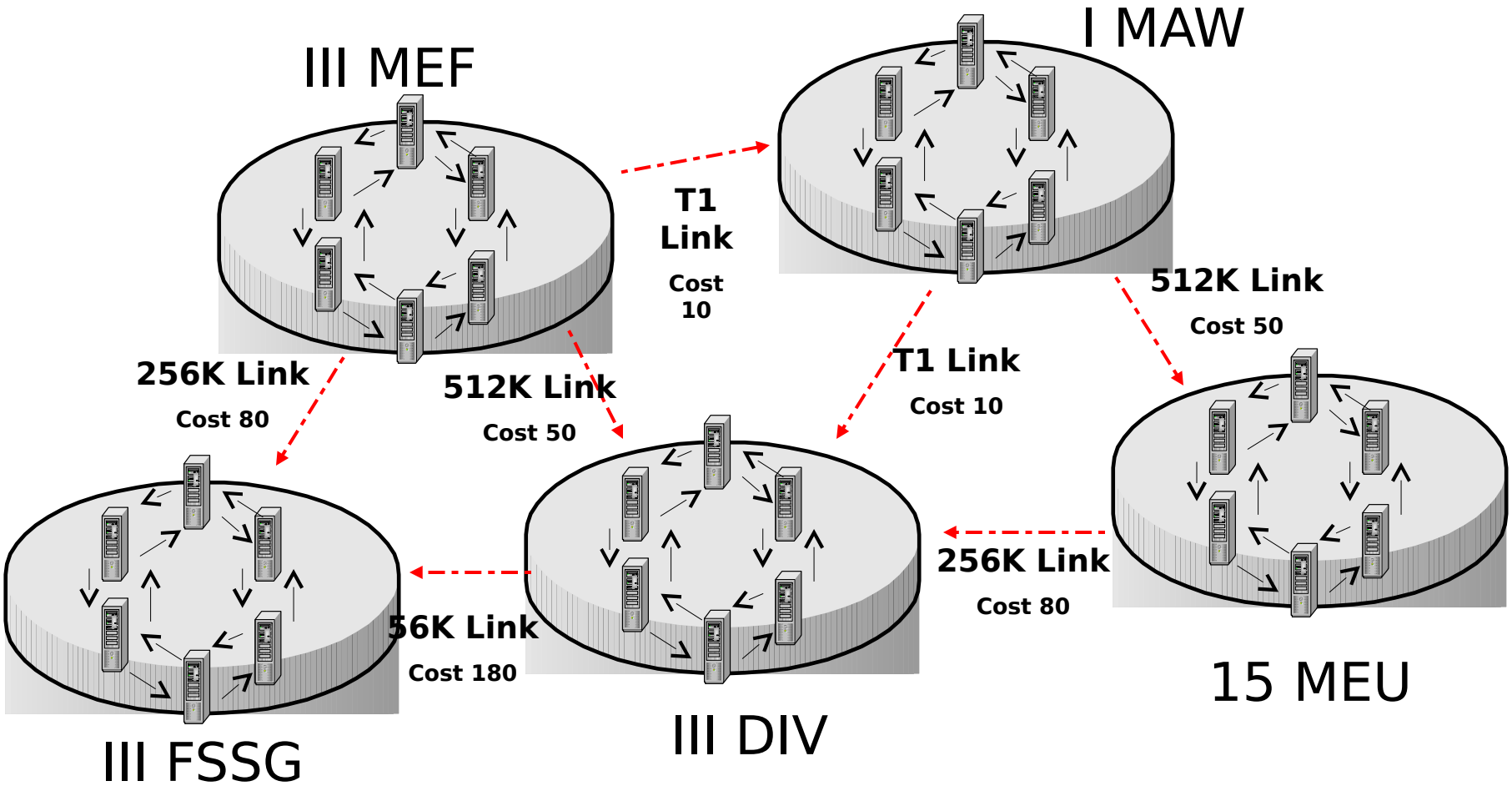
Site Links

MSTP

- Manual creation of links
  - KCC will automatically create the connection objects or you can manually create the replication link
- KCC creates what is known as a “Minimum Cost Spanning Tree”

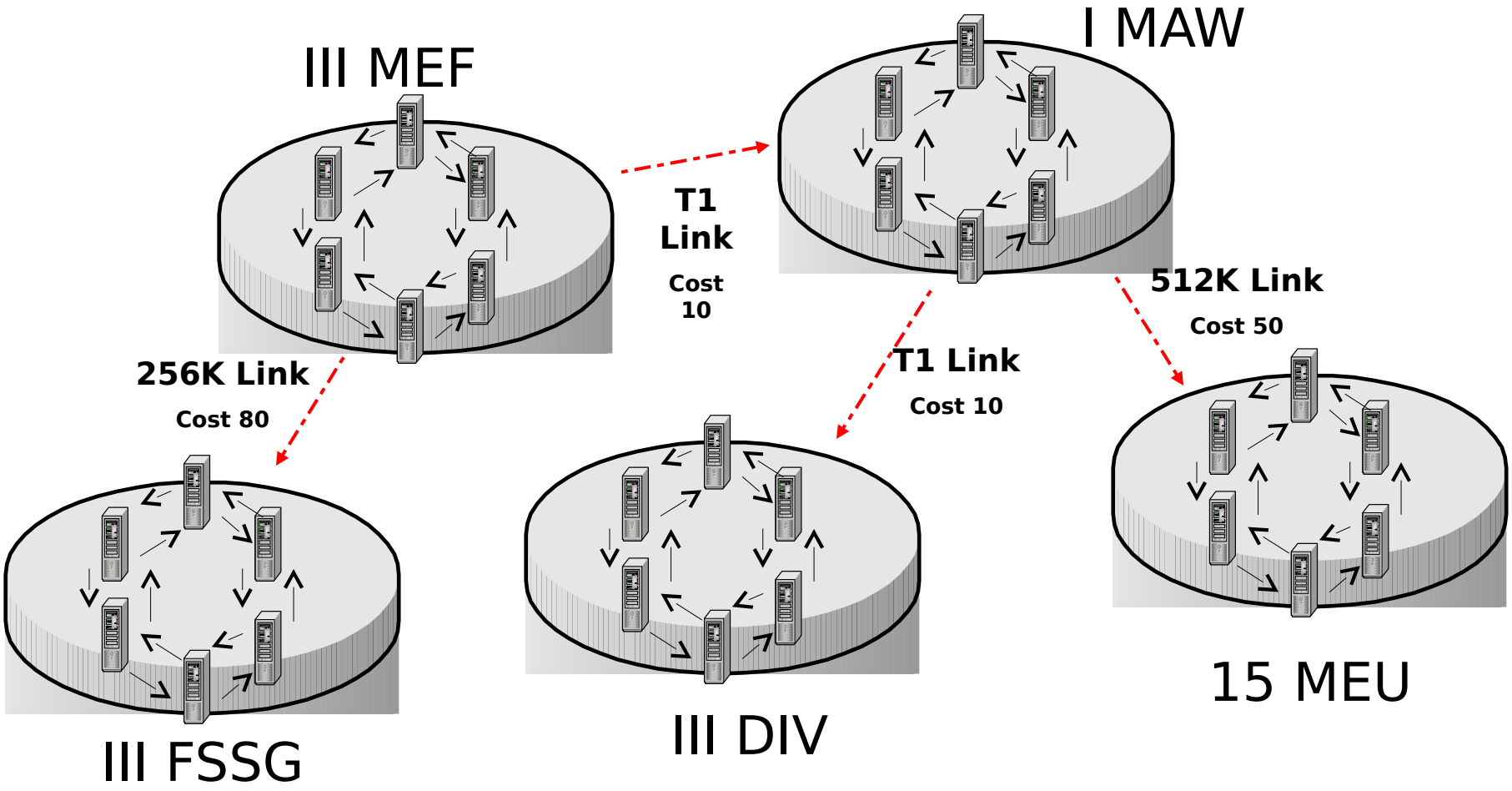
Minimum Cost Spanning Tree

MSTP



Minimum Cost Spanning Tree

MSTP



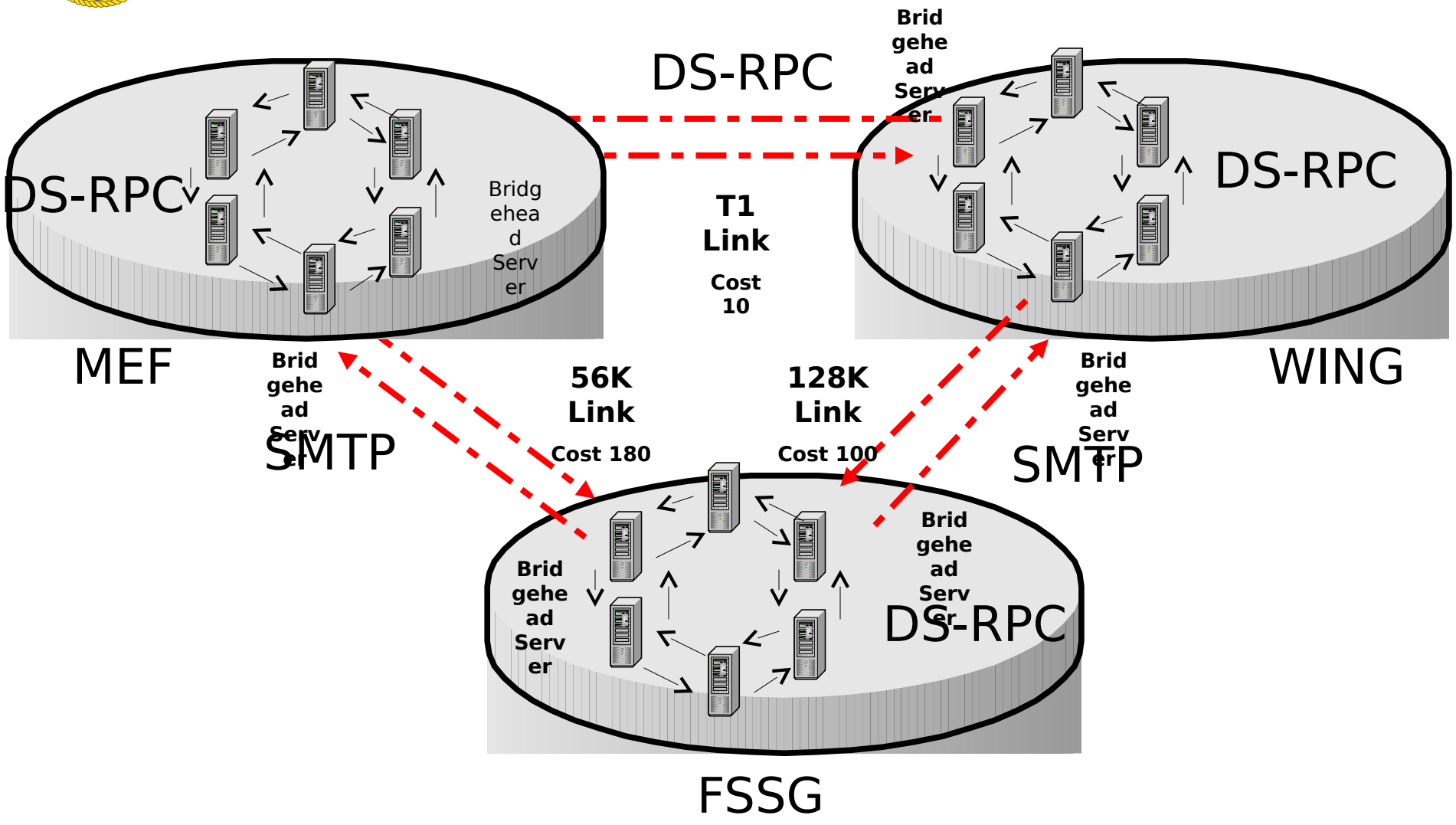
Site Link Bridges

MSTP

- The bridge knows how sites are connected
- Can be created automatically by KCC or manually by an administrator
- Knows how to route to remote sites which are not directly connected to us
- All site links on site link bridge must use the same transport protocol
- The KCC can be configured to automatically configure Bridges for all site links that use a Common Transport protocol

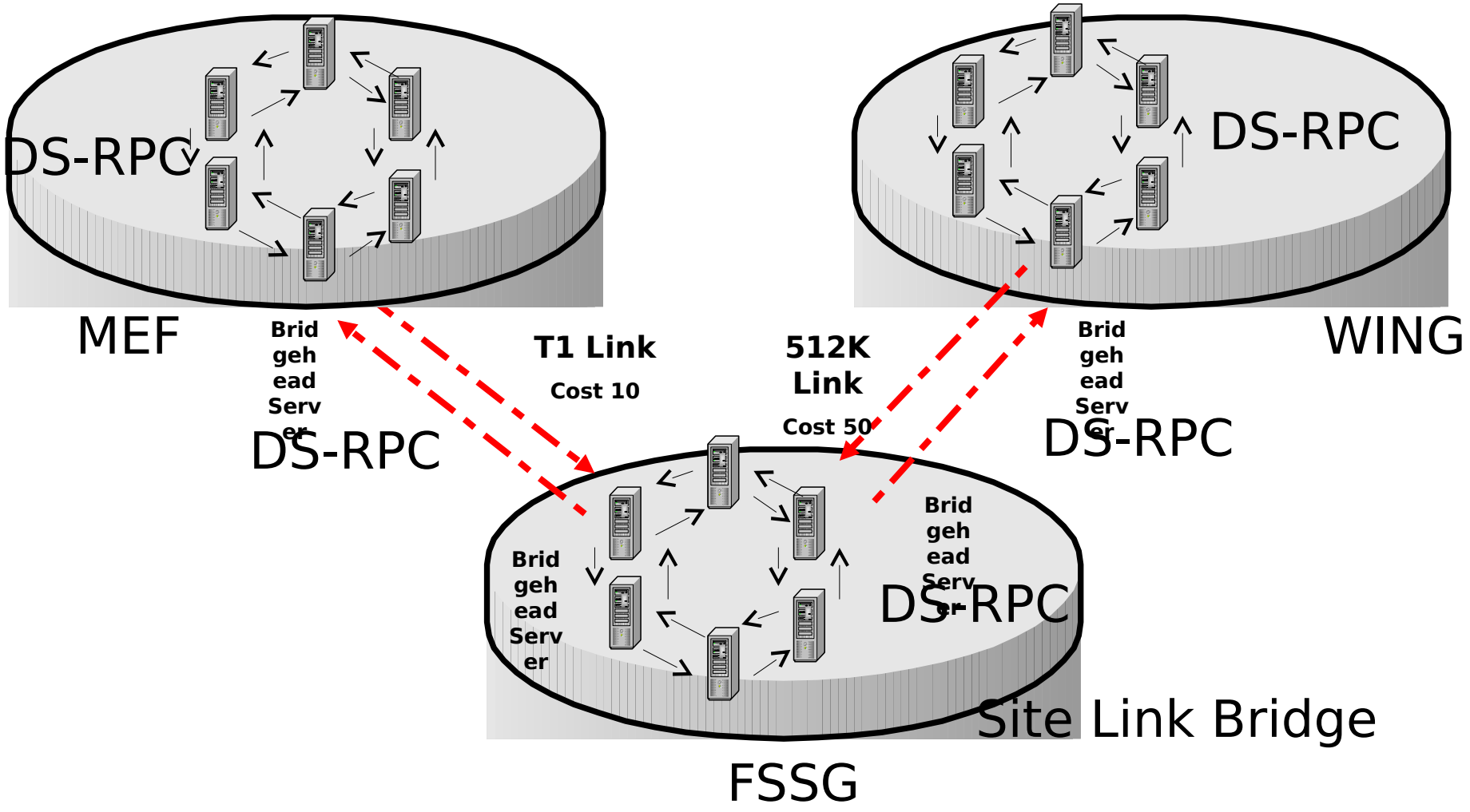
Site Links and Cost

MSTP



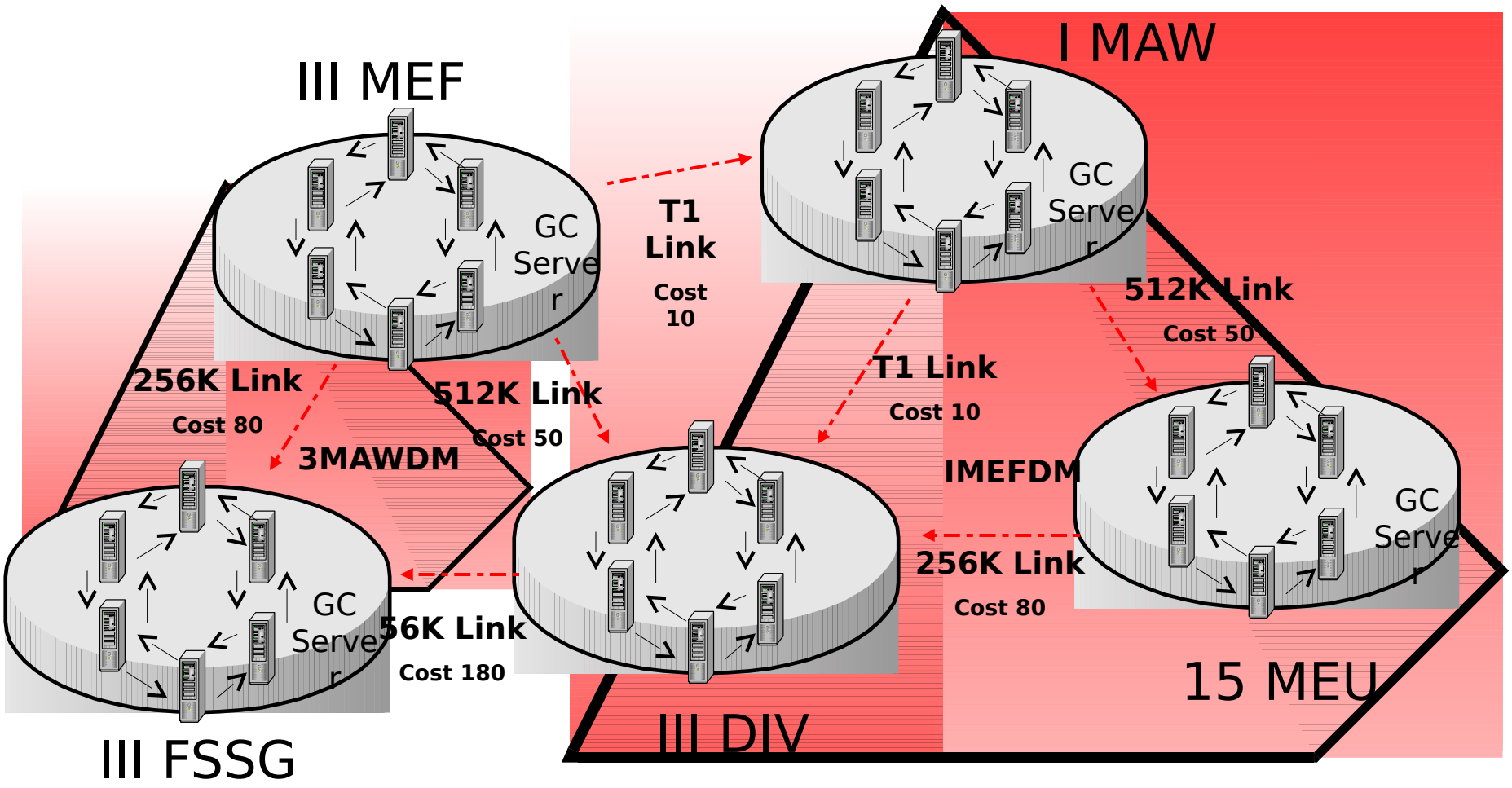
Site Link Bridges

MSTP



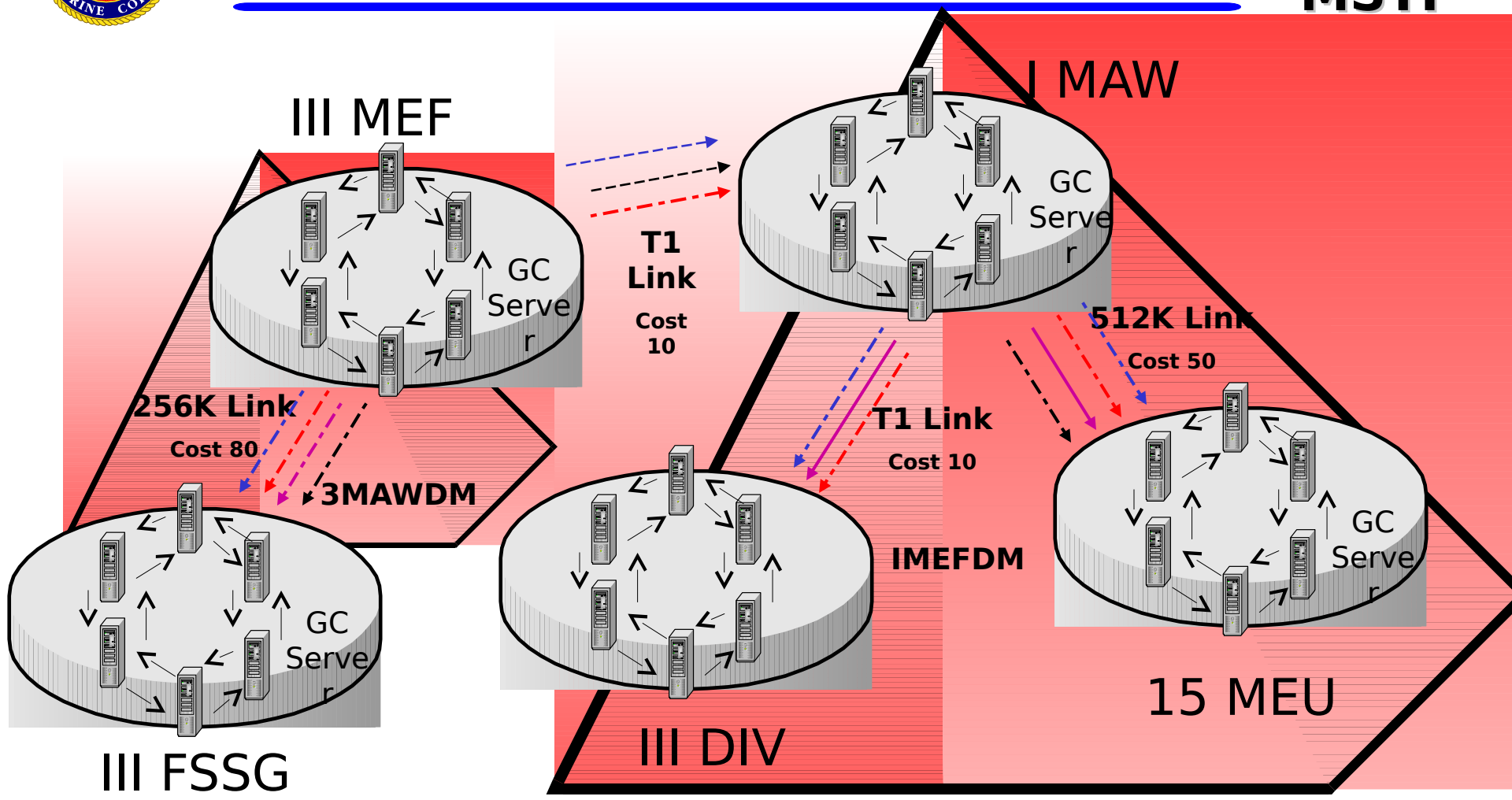
Replication Topologies

MSTP



Replication Topologies

MSTP



Site Link — Global Catalog information — Domain Information — Schema / Config information

AD Integrated Services

MSTP

- Exchange 2003

  - Deeply integrated with Active Directory and is stored in a naming context through the domain.

- Dynamic DNS (DDNS)

  - Used for location of services in AD and design of the namespace.

- Dynamic Host Configuration protocol

  - Used to configure client machines with TCP/IP information and registers clients with AD and DNS.